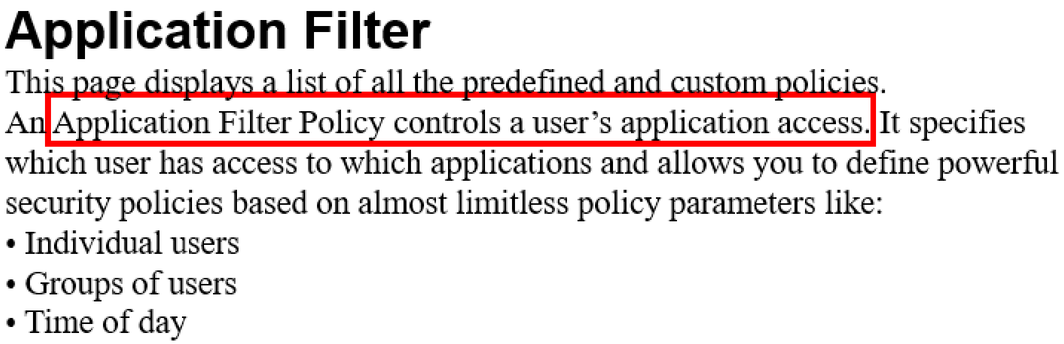
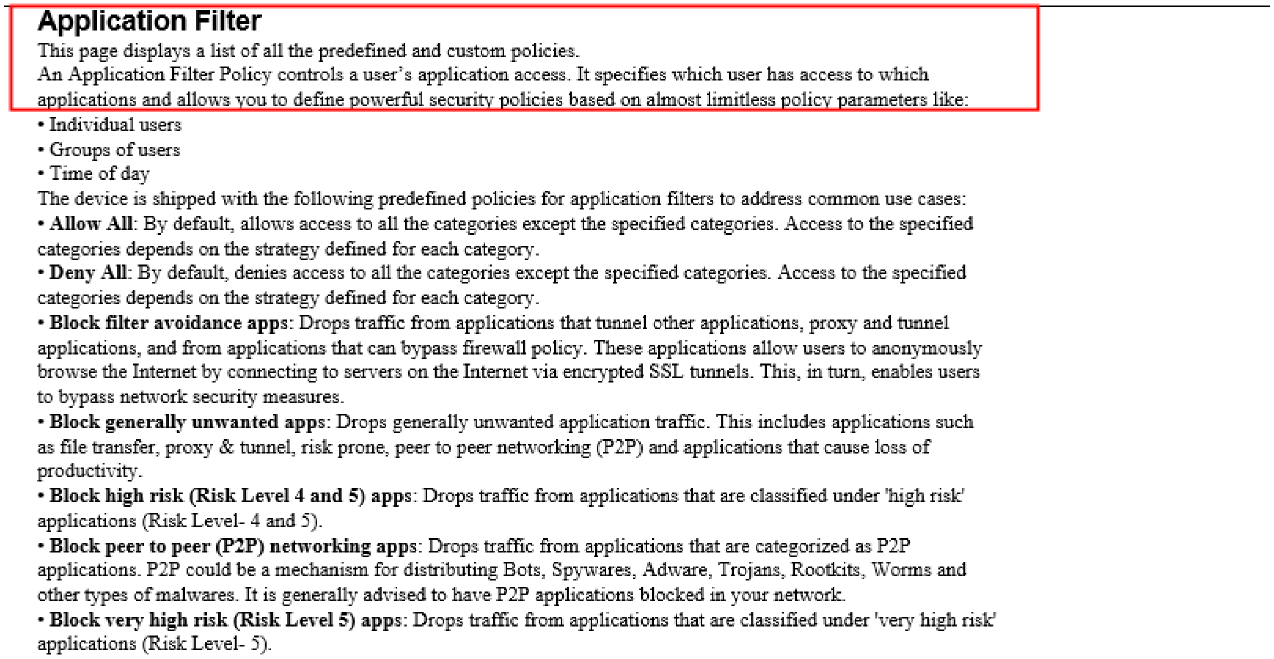
Exhibit 12

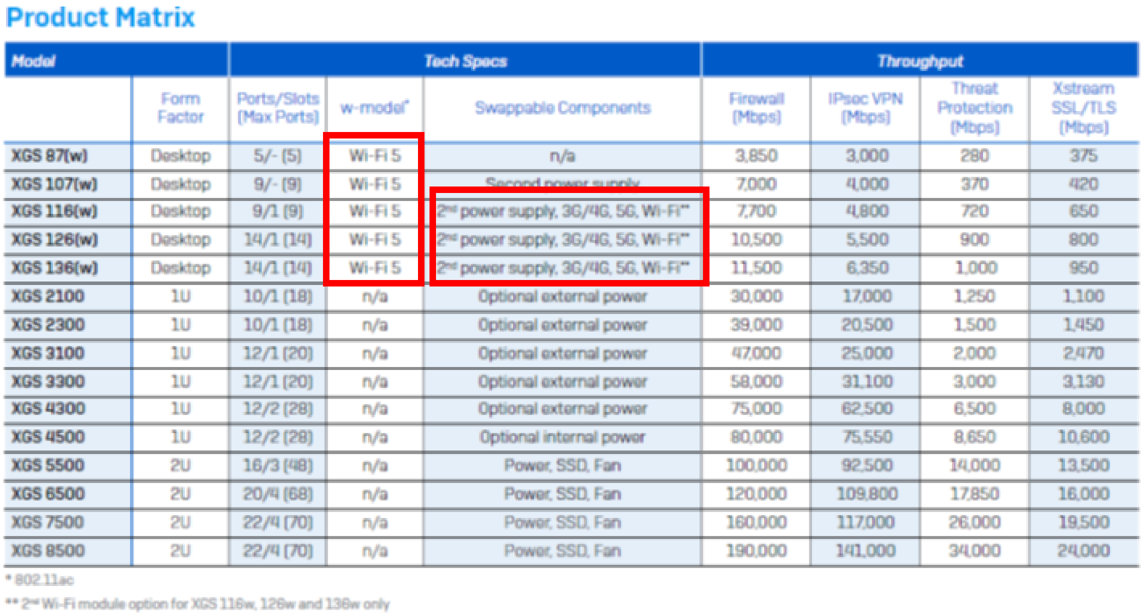
Exhibit 12 – U.S. Patent No. 8,699,999

Claims	Identification
[6pre] A method for providing security features for a mobile device, wherein the method comprises:	*Sophos XGS firewall appliances provide security features for a mobile device. For example, XGS firewall appliances control whether an application is allowed to be executed on the mobile device.*  **Application Filter** This page displays a list of all the predefined and custom policies. An Application Filter Policy controls a user's application access. It specifies which user has access to which applications and allows you to define powerful security policies based on almost limitless policy parameters like: • Individual users • Groups of users • Time of day https://utm-shop.de/media/manual/sophos-firewall-v17.0.0/docs.sophos.com/nsg/Sophos-firewall/v16056/PDF/Sophos%20XG%20Firewall%20Web%20Interface%20Reference%20Guide.pdf

Claims	**Identification**
[6a] providing a security management module with one or more security features;	*Sophos XGS firewall appliances provide a security management module (e.g., application filter) with one or more security features (e.g., control whether an application is allowed to be executed on a mobile device.)*  **Application Filter** This page displays a list of all the predefined and custom policies. An Application Filter Policy controls a user's application access. It specifies which user has access to which applications and allows you to define powerful security policies based on almost limitless policy parameters like: • Individual users • Groups of users • Time of day The device is shipped with the following predefined policies for application filters to address common use cases: • **Allow All**: By default, allows access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category. • **Deny All**: By default, denies access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category. • **Block filter avoidance apps**: Drops traffic from applications that tunnel other applications, proxy and tunnel applications, and from applications that can bypass firewall policy. These applications allow users to anonymously browse the Internet by connecting to servers on the Internet via encrypted SSL tunnels. This, in turn, enables users to bypass network security measures. • **Block generally unwanted apps**: Drops generally unwanted application traffic. This includes applications such as file transfer, proxy & tunnel, risk prone, peer to peer networking (P2P) and applications that cause loss of productivity. • **Block high risk (Risk Level 4 and 5) apps**: Drops traffic from applications that are classified under 'high risk' applications (Risk Level- 4 and 5). • **Block peer to peer (P2P) networking apps**: Drops traffic from applications that are categorized as P2P applications. P2P could be a mechanism for distributing Bots, Spywares, Adware, Trojans, Rootkits, Worms and other types of malwares. It is generally advised to have P2P applications blocked in your network. • **Block very high risk (Risk Level 5) apps**: Drops traffic from applications that are classified under 'very high risk' applications (Risk Level- 5). https://utm-shop.de/media/manual/sophos-firewall-v17.0.0/docs.sophos.com/nsg/Sophos-firewall/v16056/PDF/Sophos%20XG%20Firewall%20Web%20Interface%20Reference%20Guide.pdf

<table>
<tr><th>Claims</th><th>Identification</th></tr>
<tr>
<td>[6b] providing a connect module for updating the one or more security features;</td>
<td>

Sophos XGS firewall appliances provide a connect module (e.g., Ethernet, Wi-Fi, 3G,4G, 5G) for updating the security features (e.g., control whether an application is allowed to be executed on a mobile device.)



Product Matrix

<table>
<tr><th colspan="2">Model</th><th colspan="3">Tech Specs</th><th colspan="4">Throughput</th></tr>
<tr><th></th><th>Form Factor</th><th>Ports/Slots (Max Ports)</th><th>w-model*</th><th>Swappable Components</th><th>Firewall (Mbps)</th><th>IPsec VPN (Mbps)</th><th>Threat Protection (Mbps)</th><th>Xstream SSL/TLS (Mbps)</th></tr>
<tr><td>XGS 87(w)</td><td>Desktop</td><td>5/- (5)</td><td>Wi-Fi 5</td><td>n/a</td><td>3,850</td><td>3,000</td><td>280</td><td>375</td></tr>
<tr><td>XGS 107(w)</td><td>Desktop</td><td>9/- (9)</td><td>Wi-Fi 5</td><td>Second power supply</td><td>7,000</td><td>4,000</td><td>370</td><td>420</td></tr>
<tr><td>XGS 116(w)</td><td>Desktop</td><td>9/1 (9)</td><td>Wi-Fi 5</td><td>2nd power supply, 3G/4G, 5G, Wi-Fi**</td><td>7,700</td><td>4,800</td><td>720</td><td>650</td></tr>
<tr><td>XGS 126(w)</td><td>Desktop</td><td>14/1 (14)</td><td>Wi-Fi 5</td><td>2nd power supply, 3G/4G, 5G, Wi-Fi**</td><td>10,500</td><td>5,500</td><td>900</td><td>800</td></tr>
<tr><td>XGS 136(w)</td><td>Desktop</td><td>14/1 (14)</td><td>Wi-Fi 5</td><td>2nd power supply, 3G/4G, 5G, Wi-Fi**</td><td>11,500</td><td>6,350</td><td>1,000</td><td>950</td></tr>
<tr><td>XGS 2100</td><td>1U</td><td>10/1 (18)</td><td>n/a</td><td>Optional external power</td><td>30,000</td><td>17,000</td><td>1,250</td><td>1,100</td></tr>
<tr><td>XGS 2300</td><td>1U</td><td>10/1 (18)</td><td>n/a</td><td>Optional external power</td><td>39,000</td><td>20,500</td><td>1,500</td><td>1,450</td></tr>
<tr><td>XGS 3100</td><td>1U</td><td>12/1 (20)</td><td>n/a</td><td>Optional external power</td><td>47,000</td><td>25,000</td><td>2,000</td><td>2,470</td></tr>
<tr><td>XGS 3300</td><td>1U</td><td>12/1 (20)</td><td>n/a</td><td>Optional external power</td><td>58,000</td><td>31,100</td><td>3,000</td><td>3,130</td></tr>
<tr><td>XGS 4300</td><td>1U</td><td>12/2 (28)</td><td>n/a</td><td>Optional external power</td><td>75,000</td><td>62,500</td><td>6,500</td><td>8,000</td></tr>
<tr><td>XGS 4500</td><td>1U</td><td>12/2 (28)</td><td>n/a</td><td>Optional internal power</td><td>80,000</td><td>75,550</td><td>8,650</td><td>10,600</td></tr>
<tr><td>XGS 5500</td><td>2U</td><td>16/3 (48)</td><td>n/a</td><td>Power, SSD, Fan</td><td>100,000</td><td>92,500</td><td>14,000</td><td>13,500</td></tr>
<tr><td>XGS 6500</td><td>2U</td><td>20/4 (68)</td><td>n/a</td><td>Power, SSD, Fan</td><td>120,000</td><td>109,800</td><td>17,850</td><td>16,000</td></tr>
<tr><td>XGS 7500</td><td>2U</td><td>22/4 (70)</td><td>n/a</td><td>Power, SSD, Fan</td><td>160,000</td><td>117,000</td><td>26,000</td><td>19,500</td></tr>
<tr><td>XGS 8500</td><td>2U</td><td>22/4 (70)</td><td>n/a</td><td>Power, SSD, Fan</td><td>190,000</td><td>141,000</td><td>34,000</td><td>24,000</td></tr>
</table>

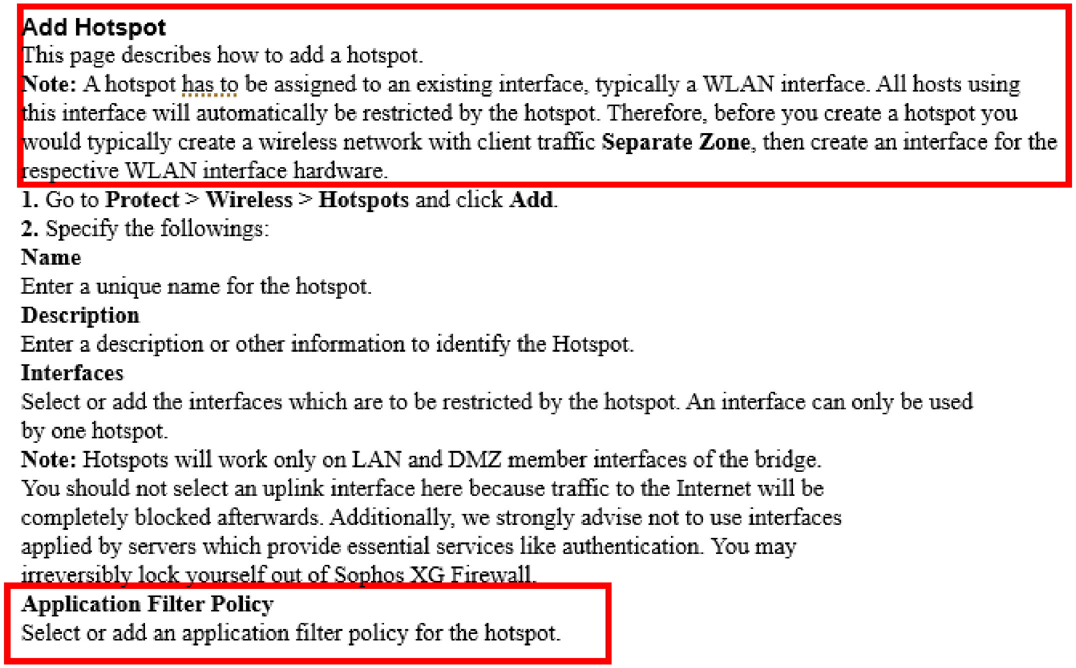
* 802.11ac

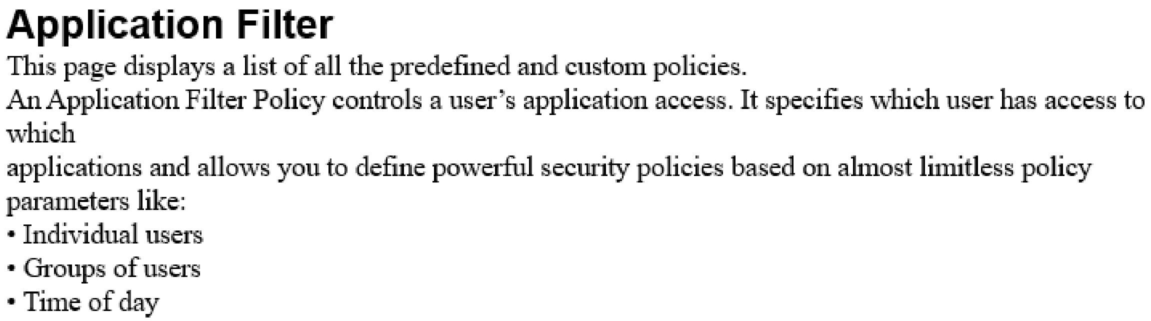
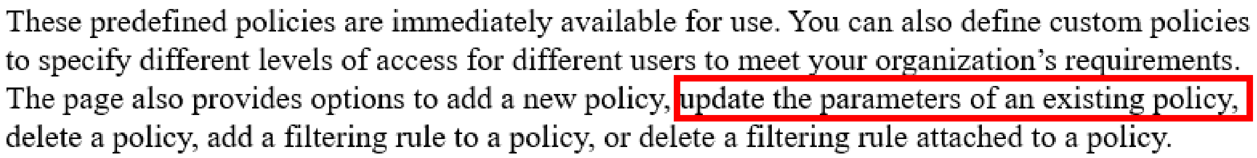
** 2nd Wi-Fi module option for XGS 116w, 126w and 136w only

https://assets.sophos.com/X24WTUEQ/at/7wf85vbnnqf939bbhtxgfk/sophos-firewall-br.pdf

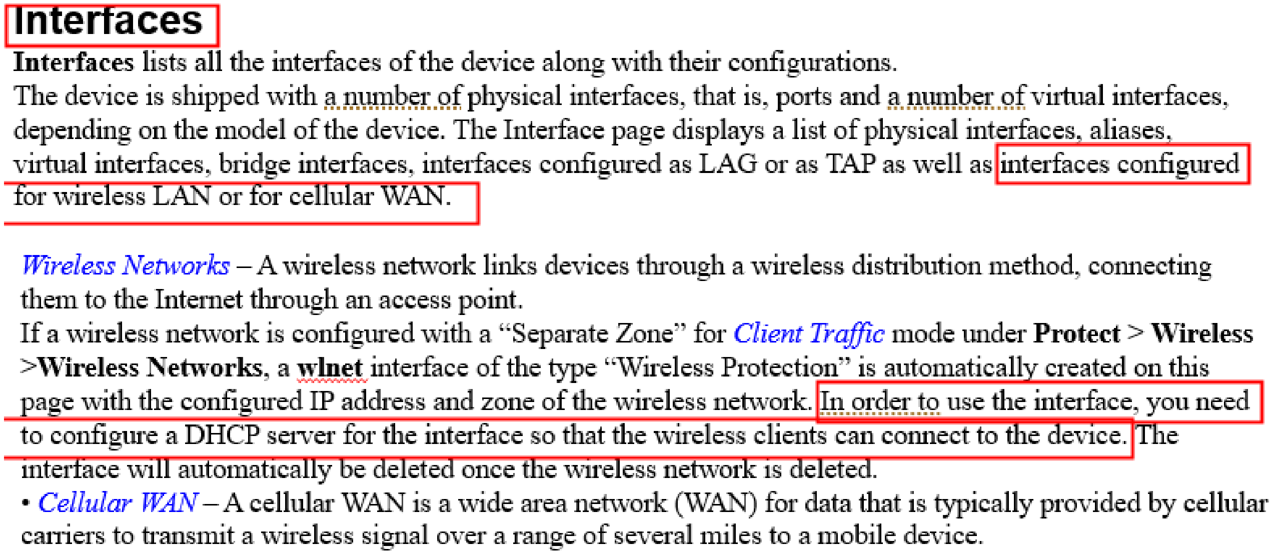
</td>
</tr>
</table>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 12 – U.S. Patent No. 8,699,999

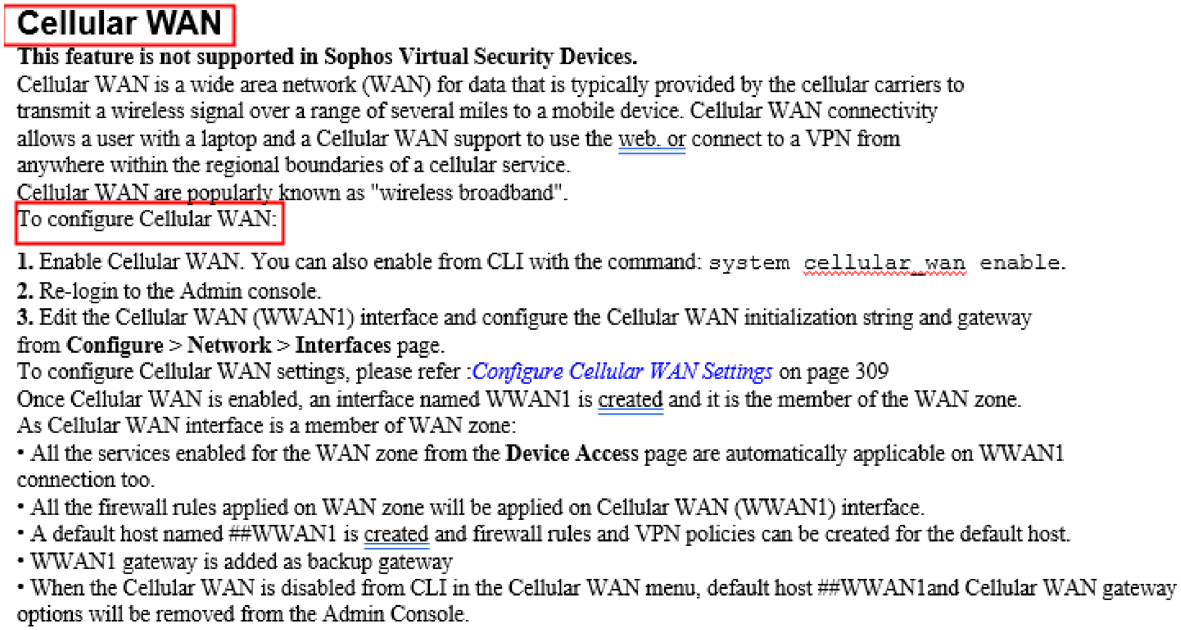
Claims	Identification
	Sophos XGS firewall appliances provide a connect module (e.g., Ethernet, WiFi, 3G,4G, 5G) for updating the security features (e.g., control whether an application is allowed to be executed on a mobile device.)  **Add Hotspot** This page describes how to add a hotspot. **Note:** A hotspot has to be assigned to an existing interface, typically a WLAN interface. All hosts using this interface will automatically be restricted by the hotspot. Therefore, before you create a hotspot you would typically create a wireless network with client traffic **Separate Zone**, then create an interface for the respective WLAN interface hardware. **1.** Go to **Protect** > **Wireless** > **Hotspots** and click **Add**. **2.** Specify the followings: **Name** Enter a unique name for the hotspot. **Description** Enter a description or other information to identify the Hotspot. **Interfaces** Select or add the interfaces which are to be restricted by the hotspot. An interface can only be used by one hotspot. **Note:** Hotspots will work only on LAN and DMZ member interfaces of the bridge. You should not select an uplink interface here because traffic to the Internet will be completely blocked afterwards. Additionally, we strongly advise not to use interfaces applied by servers which provide essential services like authentication. You may irreversibly lock yourself out of Sophos XG Firewall. **Application Filter Policy** Select or add an application filter policy for the hotspot. https://assets.sophos.com/X24WTUEQ/at/7wf85vbnnqf939bbhtxgfk/sophos-firewall-br.pdf

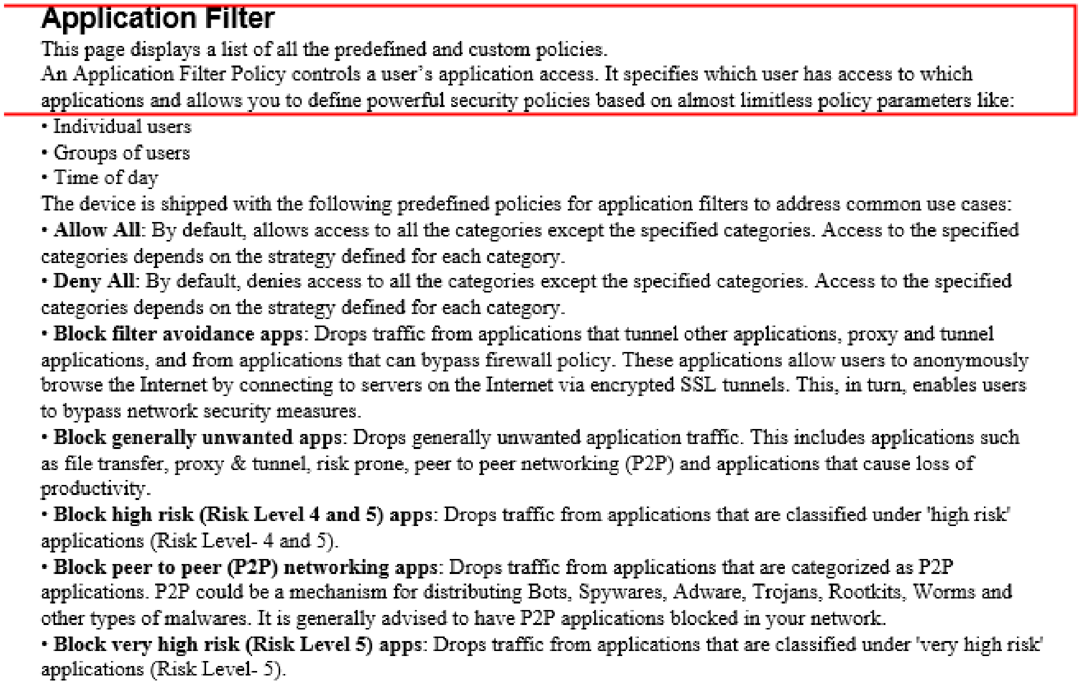
Claims	**Identification**
	Sophos XGS firewall appliances provide a connect module (e.g., Ethernet, WiFi, 3G,4G, 5G) for updating the security features (e.g., control whether an application is allowed to be executed on a mobile device.)  **Application Filter** This page displays a list of all the predefined and custom policies. An Application Filter Policy controls a user's application access. It specifies which user has access to which applications and allows you to define powerful security policies based on almost limitless policy parameters like: • Individual users • Groups of users • Time of day  These predefined policies are immediately available for use. You can also define custom policies to specify different levels of access for different users to meet your organization's requirements. The page also provides options to add a new policy, update the parameters of an existing policy, delete a policy, add a filtering rule to a policy, or delete a filtering rule attached to a policy. https://utm-shop.de/media/manual/sophos-firewall-v17.0.0/docs.sophos.com/nsg/Sophos-firewall/v16056/PDF/Sophos%20XG%20Firewall%20Web%20Interface%20Reference%20Guide.pdf

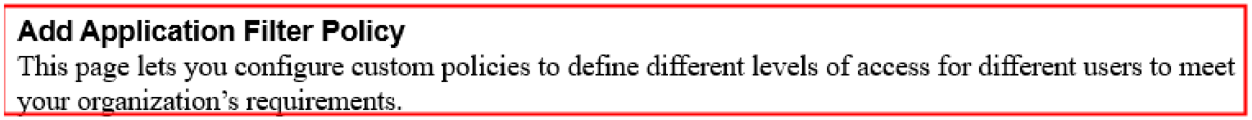
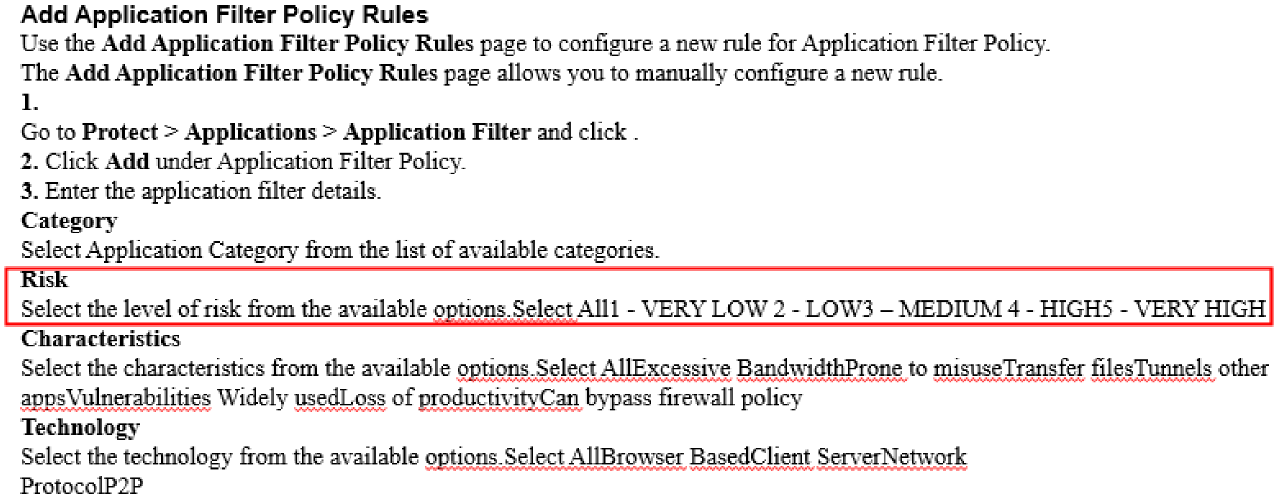
Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 12 – U.S. Patent No. 8,699,999

Claims	**Identification**
[6c] interfacing the connect module and the security management module with an operating system of the mobile device, by integrating application programming interfaces of the connect module with host environment application programming interfaces and providing security services to the mobile device via the application programming interfaces of the connect module to augment the behavior of the host environment application programming interfaces and the mobile device in order to affect the security capabilities of the operating system;	*Sophos XGS connect module (e.g., Ethernet, WiFi, 3G,4G, 5G) and security management module interface with the OS (e.g., Android, Windows, IoS) of the mobile device via APIs for updating the security features (e.g., control whether an application is allowed to be executed on a mobile device.)*  **Interfaces** **Interfaces** lists all the interfaces of the device along with their configurations. The device is shipped with a number of physical interfaces, that is, ports and a number of virtual interfaces, depending on the model of the device. The Interface page displays a list of physical interfaces, aliases, virtual interfaces, bridge interfaces, interfaces configured as LAG or as TAP as well as interfaces configured for wireless LAN or for cellular WAN. *Wireless Networks* – A wireless network links devices through a wireless distribution method, connecting them to the Internet through an access point. If a wireless network is configured with a "Separate Zone" for *Client Traffic* mode under **Protect** > **Wireless** >**Wireless Networks**, a **wlnet** interface of the type "Wireless Protection" is automatically created on this page with the configured IP address and zone of the wireless network. In order to use the interface, you need to configure a DHCP server for the interface so that the wireless clients can connect to the device. The interface will automatically be deleted once the wireless network is deleted. • *Cellular WAN* – A cellular WAN is a wide area network (WAN) for data that is typically provided by cellular carriers to transmit a wireless signal over a range of several miles to a mobile device. https://utm-shop.de/media/manual/sophos-firewall-v17.0.0/docs.sophos.com/nsg/Sophos-firewall/v16056/PDF/Sophos%20XG%20Firewall%20Web%20Interface%20Reference%20Guide.pdf

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 12 – U.S. Patent No. 8,699,999

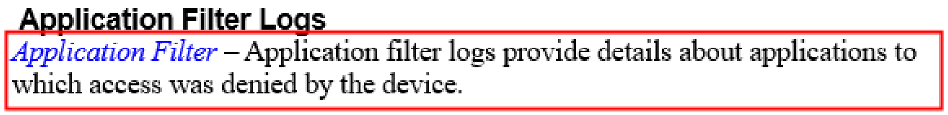
Claims	Identification
	Sophos XGS connect module (e.g., Ethernet, WiFi, 3G,4G, 5G) and security management module interface with the OS (e.g., Android, Windows, IoS) of the mobile device via APIs for updating the security features (e.g., control whether an application is allowed to be executed on a mobile device.) The connect module API is described in the cellular WAN configuration below.  **Cellular WAN** **This feature is not supported in Sophos Virtual Security Devices.** Cellular WAN is a wide area network (WAN) for data that is typically provided by the cellular carriers to transmit a wireless signal over a range of several miles to a mobile device. Cellular WAN connectivity allows a user with a laptop and a Cellular WAN support to use the web. or connect to a VPN from anywhere within the regional boundaries of a cellular service. Cellular WAN are popularly known as "wireless broadband". To configure Cellular WAN: **1.** Enable Cellular WAN. You can also enable from CLI with the command: `system cellular_wan enable`. **2.** Re-login to the Admin console. **3.** Edit the Cellular WAN (WWAN1) interface and configure the Cellular WAN initialization string and gateway from **Configure** > **Network** > **Interfaces** page. To configure Cellular WAN settings, please refer :*Configure Cellular WAN Settings* on page 309 Once Cellular WAN is enabled, an interface named WWAN1 is created and it is the member of the WAN zone. As Cellular WAN interface is a member of WAN zone: • All the services enabled for the WAN zone from the **Device Access** page are automatically applicable on WWAN1 connection too. • All the firewall rules applied on WAN zone will be applied on Cellular WAN (WWAN1) interface. • A default host named ##WWAN1 is created and firewall rules and VPN policies can be created for the default host. • WWAN1 gateway is added as backup gateway • When the Cellular WAN is disabled from CLI in the Cellular WAN menu, default host ##WWAN1and Cellular WAN gateway options will be removed from the Admin Console. https://utm-shop.de/media/manual/sophos-firewall-v17.0.0/docs.sophos.com/nsg/Sophos-firewall/v16056/PDF/Sophos%20XG%20Firewall%20Web%20Interface%20Reference%20Guide.pdf

Claims	Identification
	Sophos XGS appliances provide security services to the mobile device by filtering applications allowed to execute on the mobile device via the connect module management module API. The application filter augments the OS of the mobile device by denying execution of high risk (e.g., malicious) applications on the mobile device.  **Application Filter** This page displays a list of all the predefined and custom policies. An Application Filter Policy controls a user's application access. It specifies which user has access to which applications and allows you to define powerful security policies based on almost limitless policy parameters like: • Individual users • Groups of users • Time of day The device is shipped with the following predefined policies for application filters to address common use cases: • **Allow All**: By default, allows access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category. • **Deny All**: By default, denies access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category. • **Block filter avoidance apps**: Drops traffic from applications that tunnel other applications, proxy and tunnel applications, and from applications that can bypass firewall policy. These applications allow users to anonymously browse the Internet by connecting to servers on the Internet via encrypted SSL tunnels. This, in turn, enables users to bypass network security measures. • **Block generally unwanted apps**: Drops generally unwanted application traffic. This includes applications such as file transfer, proxy & tunnel, risk prone, peer to peer networking (P2P) and applications that cause loss of productivity. • **Block high risk (Risk Level 4 and 5) apps**: Drops traffic from applications that are classified under 'high risk' applications (Risk Level- 4 and 5). • **Block peer to peer (P2P) networking apps**: Drops traffic from applications that are categorized as P2P applications. P2P could be a mechanism for distributing Bots, Spywares, Adware, Trojans, Rootkits, Worms and other types of malwares. It is generally advised to have P2P applications blocked in your network. • **Block very high risk (Risk Level 5) apps**: Drops traffic from applications that are classified under 'very high risk' applications (Risk Level- 5). https://utm-shop.de/media/manual/sophos-firewall-v17.0.0/docs.sophos.com/nsg/Sophos-firewall/v16056/PDF/Sophos%20XG%20Firewall%20Web%20Interface%20Reference%20Guide.pdf

Claims	Identification
[6d] providing execution information to the security management module, the execution information comprising information on whether an application on the mobile device is allowed to be executed by the operating system; and	*Sophos XGS firewall provides execution information (e.g., application allowed or denied) to the security management module on whether the application is allowed to be executed by the operating system. The application is allowed or denied based on a risk level associated with the application.*  **Add Application Filter Policy** This page lets you configure custom policies to define different levels of access for different users to meet your organization's requirements.  **Add Application Filter Policy Rules** Use the **Add Application Filter Policy Rules** page to configure a new rule for Application Filter Policy. The **Add Application Filter Policy Rules** page allows you to manually configure a new rule. **1.** Go to **Protect** > **Applications** > **Application Filter** and click . **2.** Click **Add** under Application Filter Policy. **3.** Enter the application filter details. **Category** Select Application Category from the list of available categories. **Risk** Select the level of risk from the available options.Select All1 - VERY LOW 2 - LOW3 – MEDIUM 4 - HIGH5 - VERY HIGH **Characteristics** Select the characteristics from the available options.Select AllExcessive BandwidthProne to misuseTransfer filesTunnels other appsVulnerabilities Widely usedLoss of productivityCan bypass firewall policy **Technology** Select the technology from the available options.Select AllBrowser BasedClient ServerNetwork ProtocolP2P https://utm-shop.de/media/manual/sophos-firewall-v17.0.0/docs.sophos.com/nsg/Sophos-firewall/v16056/PDF/Sophos%20XG%20Firewall%20Web%20Interface%20Reference%20Guide.pdf

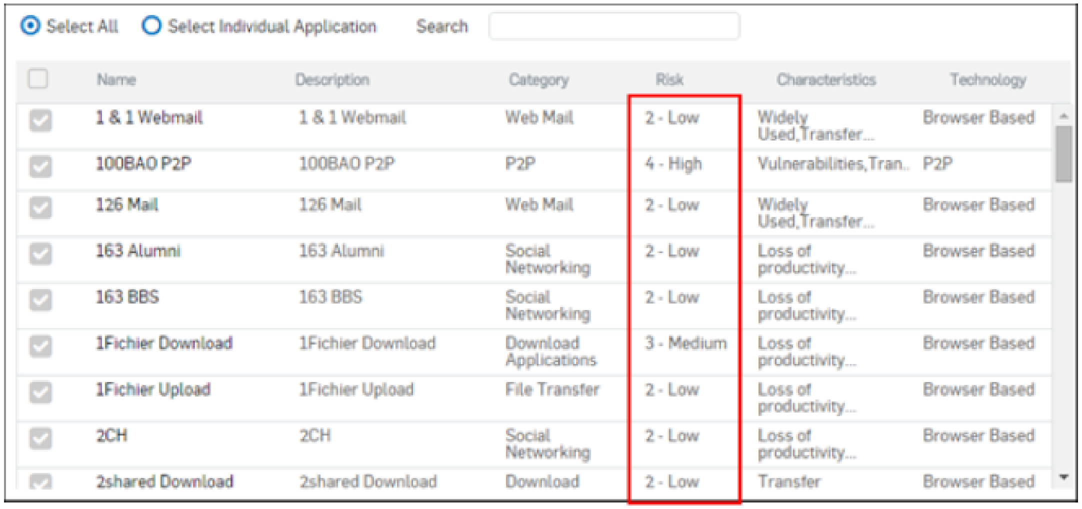
<table>
<tr><th>Claims</th><th>Identification</th></tr>
<tr>
<td>[6e] when a given application is to be executed on the mobile device, allowing execution of the given application when the execution information indicates that the given application is an allowable application, and otherwise not allowing execution of the given application.</td>
<td>

Sophos XGS allows application execution when the execution information does not deny the application access. For example, applications with low risk levels are allowed.



Application Filter Logs

Application Filter – Application filter logs provide details about applications to which access was denied by the device.



● Select All ○ Select Individual Application Search

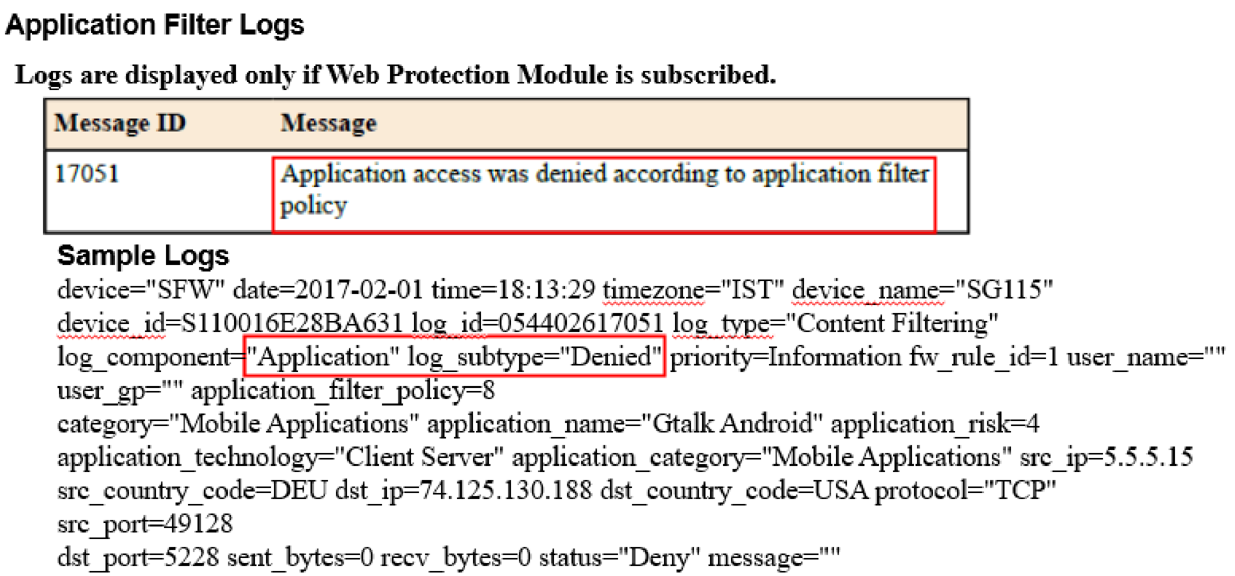
<table>
<tr><th>□</th><th>Name</th><th>Description</th><th>Category</th><th>Risk</th><th>Characteristics</th><th>Technology</th></tr>
<tr><td>☑</td><td>1 &amp; 1 Webmail</td><td>1 &amp; 1 Webmail</td><td>Web Mail</td><td>2 - Low</td><td>Widely Used,Transfer...</td><td>Browser Based</td></tr>
<tr><td>☑</td><td>100BAO P2P</td><td>100BAO P2P</td><td>P2P</td><td>4 - High</td><td>Vulnerabilities,Tran...</td><td>P2P</td></tr>
<tr><td>☑</td><td>126 Mail</td><td>126 Mail</td><td>Web Mail</td><td>2 - Low</td><td>Widely Used,Transfer...</td><td>Browser Based</td></tr>
<tr><td>☑</td><td>163 Alumni</td><td>163 Alumni</td><td>Social Networking</td><td>2 - Low</td><td>Loss of productivity...</td><td>Browser Based</td></tr>
<tr><td>☑</td><td>163 BBS</td><td>163 BBS</td><td>Social Networking</td><td>2 - Low</td><td>Loss of productivity...</td><td>Browser Based</td></tr>
<tr><td>☑</td><td>1Fichier Download</td><td>1Fichier Download</td><td>Download Applications</td><td>3 - Medium</td><td>Loss of productivity...</td><td>Browser Based</td></tr>
<tr><td>☑</td><td>1Fichier Upload</td><td>1Fichier Upload</td><td>File Transfer</td><td>2 - Low</td><td>Loss of productivity...</td><td>Browser Based</td></tr>
<tr><td>☑</td><td>2CH</td><td>2CH</td><td>Social Networking</td><td>2 - Low</td><td>Loss of productivity...</td><td>Browser Based</td></tr>
<tr><td>☑</td><td>2shared Download</td><td>2shared Download</td><td>Download</td><td>2 - Low</td><td>Transfer</td><td>Browser Based</td></tr>
</table>

https://utm-shop.de/media/manual/sophos-firewall-v17.0.0/docs.sophos.com/nsg/Sophos-firewall/v16056/PDF/Sophos%20XG%20Firewall%20Web%20Interface%20Reference%20Guide.pdf

</td>
</tr>
</table>

Malikie Innovations Ltd. and Key Patent Innovations Ltd. v. Sophos Ltd.
Exhibit 12 – U.S. Patent No. 8,699,999

Claims	**Identification**
	Sophos XGS firewall does not allow application execution when the execution information denies the application access. In the example below, the "Gtalk Android" application was denied based on an application risk level of 4.



Application Filter Logs

Logs are displayed only if Web Protection Module is subscribed.

Message ID	Message
17051	Application access was denied according to application filter policy

Sample Logs

```
device="SFW" date=2017-02-01 time=18:13:29 timezone="IST" device_name="SG115"
device_id=S110016E28BA631 log_id=054402617051 log_type="Content Filtering"
log_component="Application" log_subtype="Denied" priority=Information fw_rule_id=1 user_name=""
user_gp="" application_filter_policy=8
category="Mobile Applications" application_name="Gtalk Android" application_risk=4
application_technology="Client Server" application_category="Mobile Applications" src_ip=5.5.5.15
src_country_code=DEU dst_ip=74.125.130.188 dst_country_code=USA protocol="TCP"
src_port=49128
dst_port=5228 sent_bytes=0 recv_bytes=0 status="Deny" message=""
```

https://utm-shop.de/media/manual/sophos-firewall-v17.0.0/docs.sophos.com/nsg/Sophos-firewall/v16056/PDF/Sophos%20XG%20Firewall%20Web%20Interface%20Reference%20Guide.pdf